UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/662,072	09/14/2000	John Border	PD-200053	1446

20991 7590 06/09/2009

THE DIRECTV GROUP, INC.
PATENT DOCKET ADMINISTRATION
CA / LA1 / A109
2230 E. IMPERIAL HIGHWAY
EL SEGUNDO, CA 90245

EXAMINER	
EL CHANTI, HUSSEIN A	
ART UNIT	**PAPER NUMBER**
2457	

MAIL DATE	DELIVERY MODE
06/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/662,072
Filing Date: September 14, 2000
Appellant(s): BORDER ET AL.

Phouphanomketh Ditthavong (Reg. No. 44658)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed April 2, 2009 appealing from the Office action mailed July 29, 2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Yates et al., U.S. Patent No. 6,167,438 (Dec. 26, 2000)

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

- Claims 3, 5-19-29, 32 and 34-59 are rejected under 35 U.S.C. 102(e) as being anticipated by Yates et al., U.S. Patent No. 6,167,438 (referred to hereafter as Yates).

As to claims 3 and 32, Yates teaches a network apparatus and method comprising:

a proxy which facilitates communication with other network entities by performing at least one performance enhancing function, the proxy communicating with the other network entities via a first type of connection and other network entities via a second type of connection (see col. 3 lines 52-col. 4 lines 8, col. 7 lines 64-col. 8 lines 13).

the proxy establishes multiple connections of the first type associated with different applications and includes:

a spoofing element, configured to intercept and alter a data flow within one of the connections to add or delete from the data flow to reduce startup latency which only spoofs connections of the first type associated with at least one of applications with high throughput and applications for which reduced startup latency is desired (see col. 4 lines 62-col. 5 lines 11 and col. 9 lines 60-col. 10 lines 30);

a multiplexing element configured to selectively multiplex the spoofed connections onto a single connection of the second type (see col. 9 lines 54-col. 10 lines 30).

As to claims 5 and 34, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein said spoofing element assigns spoofing resources including

buffer space and control blocks to the spoofed connections (see col. 9 lines 60-col. 10 lines 30).

As to claims 6 and 35, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein said spoofing element spoofs connections using at least one spoofing rule based on destination address, source address, destination port number, source port number, options, a differentiated services (DS) field or combinations thereof (see col. 14 lines 20-col. 16 lines 65).

As to claims 7 and 36, Yates teaches the apparatus and method of claims 6 and 35 respectively wherein said spoofing element defines the at least one spoofing rule in a spoofing profile (see col. 9 lines 60-col. 10 lines 30).

As to claims 8 and 37, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein the spoofing element spoofs ACKs (see col. 9 lines 15-34).

As to claims 9 and 38, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein the spoofing element spoofs a tree-way handshake (see col. 9 lines 15-34).

As to claims 10 and 39, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein the proxy includes:

a protocol element which multiplexes multiple connections of the first type onto a single connection of the second type (see col. 9 lines 35-52).

As to claims 11 and 40, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein the proxy includes:

a prioritization element which prioritizes connections of the first type to determine what priority level of the connection of the second type, each of the connections of the first type are assigned (see col. 14-col. 16).

As to claims 12 and 41, Yates teaches the apparatus and method of claims 11 and 32 respectively 41wherein said prioritizing element prioritizes connections using at least one prioritizing rule based on destination address, source address, destination port number, source port number, a differentiated services (DS) field, a type of data contained within the connection or combinations thereof (see col. 9 lines 60-col. 10 lines 30 and col. 14 lines 35-col. 16 lines 60).

As to claims 13 and 42, Yates teaches the apparatus and method of claims 12 and 41 respectively wherein said prioritizing element defines the at least one prioritizing rule in a prioritizing profile (see col. 9 lines 60-col. 10 lines 30 and col. 14 lines 35-col. 16 lines 60).

As to claims 14 and 43, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein the proxy includes:

a path selection element which selects a path for data associated with connections of the first type across connections of the second type or connections of other types (see col. 10 lines 31-63).

As to claims 15 and 44, Yates teaches the apparatus and method of claims 14 and 43 respectively wherein said path selection element can select up to N paths (N>1) where the Nth path is selected only if the (N-1) path fails (see col. 28 lines 26-30).

As to claims 16 and 45, Yates teaches the apparatus and method of claims 15 and 44 respectively wherein said path selection element selects a path using at least one path selection rule based on priority, destination address, source address, destination port number, source port number, protocol, a differentiated services (DS) field or combinations thereof (see col. 9 lines 60-col. 10 lines 30 and col. 14 lines 35-col. 16 lines 60).

As to claims 17 and 46, Yates teaches the apparatus and method of claims 16 and 45 respectively wherein said spoofing element defines the at least one path selection rule in a path selection profile (see col. 9 lines 60-col. 10 lines 30 and col. 14 lines 35-col. 16 lines 60).

As to claims 18 and 47, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein the proxy includes:

a compression/encryption element, which compresses and/or encrypts data associated with connections of the first type for transmission across connections of the second type (see col. 18 lines 21-36).

As to claims 19 and 48, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein the first connection uses a high layer protocol (see col. 9 lines 15-23).

As to claims 20 and 49, Yates teaches the apparatus and method wherein the first connection uses one of the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) (see col. 12 lines 24-38).

As to claims 21 and 50, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein the second connection is a backbone connection (see fig. 1).

As to claims 22 and 51, Yates teaches the apparatus and method of claims 3 and 32 respectively where is the connection is a wireless link (see col. 5 lines 59-col. 6 lines 2).

As to claims 23 and 52, Yates teaches the apparatus and method of claims 22 and 51 respectively, wherein the wireless link has high latency and high error rate (see col. 5 lines 59-col. 6 lines 2).

As to claims 24 and 53, Yates teaches the apparatus and method of claims 22 and 51 respectively wherein the wireless link is a satellite link (see col. 5 lines 59-col. 6 lines 2).

As to claims 25 and 54, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein said network apparatus is a component of a network gateway (see fig. 1).

As to claims 26 and 55, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein said network apparatus is a component of a host (see col. 9 lines 30-65).

As to claims 27 and 56, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein said network apparatus is a component of a hub (see col. 6 lines 1-col. 7 lines 54).

As to claims 28 and 57, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein the network apparatus is a component of a VSAT (see col. 5 lines 59-col. 6 lines 2).

As to claims 29 and 58, Yates teaches the apparatus and method of claims 3 and 32 respectively wherein said network apparatus is a component of a router (see col. 9 lines 30-65).

As to claim 59, Yates teaches the method of claim 32 wherein the method is performed in a switch (see col. 9 lines 30-65).

(10) Response to Argument

As per appellant arguments, the appellant argues that Yates does not disclose a multiplexing element configured to selectively multiplex the spoofed connections onto a single connection of the second type (see brief pages 5 lines 13-page 7 lines 16, argument A).

In reply to A, Yates teaches a system and method for establishing a connection between a client and a server through a router where the router has a snooper application capable of spoofing client requests and establishing connections to servers to obtain requested content (see col. 8 lines 55-col. 9 lines 59).

Yates teaches the router establishing a connection between the client and a cache server. The router has a snooper that identify whether a packet received from a client is a {SYN} packet or a {GET} packet. If the packet is a {SYN} packet, then the snooper spoofs the server connection until a {GET} packet is received (see col. 9 lines 54-col. 10 lines 3). The snooper monitors the connection for a {GET} message. When a

{GET} message is received, the router combines the SYN and GET message into a single {SYN+GET} message. The message is sent on a separate connection to a cache server to service the request (see col. 10 lines 16-col. 11 lines 55).

Therefore, Yates teaches the snooper "spoofing element" which intercepts connections that has {SYN} messages “connection of a first type" and spoofs the connection. Once a {GET} message is received, the router “multiplexing element” combines the SYN and GET message “multiplexing” onto a single connection with a single {SYN+GET} request "single connection of the second type”.

Examiner interprets the connection between the client and the router to be "first type of connection" where the snooper on the router receives GET messages and spoofs the connection. Examiner also interprets the connection that is established between the router and the cache server as the “second type of connection” which is used to send a combined {SYN+GET} request to the cache server.

The term “multiplex” in the broadest interpretation may be defined as “simultaneously combining multiple messages onto a single connection". Yates teaches combining a SYN and a GET message into a single {SYN+GET} message which is sent through a cache server through an established session. In addition, the claim language states “a spoofing element configured to intercept and alter a data flow within *one of the connections*” and “multiplex the spoofed connections onto a single connection of the second type”. As evident by the claim language, the spoofed connections may be a single connection. Therefore, combining messages on a first connection into a single message on a single connection of the second type as taught by Yates meets the scope

of the claimed limitation "selectively multiplex the spoofed connections onto a single connection of the second type".

Appellant argues that Yates does not disclose spoofing connections of the first type (see brief page 7 lines 15-page 8 lines 8, argument B).

In reply to B, Yates teaches the snooper "spoofing element" which intercepts connections that has {SYN} messages "connection of a first type" and spoofs the connection. Once a {GET} message is received, the router "multiplexing element" combines the SYN and GET message "multiplexing" onto a single connection with a single {SYN+GET} request "single connection of the second type".

Examiner interprets the connection between the client and the router to be "first type of connection" where the snooper on the router receives GET messages and spoofs the connection. Therefore Yates teaches "spoofing connections of the first type".

Appellant argues that Yates does not disclose a prioritizing profile or a spoofing profile with a set of rules (see brief pages 8 lines 10-page 9, argument C).

In reply to C, Yates teaches a receiving {GET} messages where the {GET} messages is routed in accordance with neighborhood information "set of rules" in a current routing tree "spoofing profile". In response to the determination of the neighborhood information in a tree the snooper selects a cache server to forward the request messages to (see col. 13 lines 17-50). Therefore Yates teaches "prioritization and a spoofing profile with a set of rules" as claimed.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Hussein Elchanti/

Patent Examiner

June 2, 2009

Conferees:

/ARIO ETIENNE/

Supervisory Patent Examiner, Art Unit 2457

/Salad Abdullahi/

Primary Examiner, Art Unit 2457